Discrete Mathematics 338 (2015) 2197–2211

Contents lists available at ScienceDirect

Discrete Mathematics

journal homepage: www.elsevier.com/locate/disc

Circulant matrices and affine equivalence of monomial rotation symmetric Boolean functions

David Canright, Jong H. Chung [1], Pantelimon Stănică *

Department of Applied Mathematics, Naval Postgraduate School, Monterey, CA 93943-5216, USA

ARTICLE INFO

Article history:
Received 30 April 2014
Received in revised form 15 October 2014
Accepted 17 May 2015

Keywords:
Boolean functions
Circulant matrices
Affine equivalence
Permutations

ABSTRACT

The goal of this paper is two-fold. We first focus on the problem of deciding whether two monomial rotation symmetric (MRS) Boolean functions are affine equivalent via a permutation. Using a correspondence between such functions and circulant matrices, we give a simple necessary and sufficient condition. We connect this problem with the well known Ádám's conjecture from graph theory. As applications, we reprove easily several main results of Cusick et al. on the number of equivalence classes under permutations for MRS in prime power dimensions, as well as give a count for the number of classes in pq number of variables, where p, q are prime numbers with $p < q < p^2$. Also, we find a connection between the generalized inverse of a circulant matrix and the invertibility of its generating polynomial over $\mathbb{F}_2$, modulo a product of cyclotomic polynomials, thus generalizing a known result on nonsingular circulant matrices.

Published by Elsevier B.V.

1. Introduction

The class of rotation symmetric Boolean functions (RSBFs) has received some attention from a combinatorial and cryptographic perspective. The initial study on the nonlinearity of these functions (called idempotents there) was done by Filiol and Fontaine [19]. Later on, the nonlinearity and correlation immunity of such functions have been studied in detail in [9,23,31,30,37,38]. Applications of such functions in hashing has also been investigated by Pieprzyk and Qu [35]. We want to mention also several papers [15–17,19,36] dealing with some other properties of RSBF, as well as their involvement in S-boxes. These functions are interesting to look into, since their space is much smaller ($\approx 2^{\frac{2^n}{n}}$) than the total space of Boolean functions (2^{2^n}) and the set contains functions with good cryptographic properties. It has been experimentally demonstrated that there are functions in this class which are good in terms of balancedness, nonlinearity, correlation immunity, algebraic degree and algebraic immunity (resistance against algebraic attack) [16].

It is interesting to note that the famous Patterson–Wiedemann functions [33] that achieve nonlinearity 16,276 (strictly greater than nonlinearity $2^{15-1} - 2^{(15-1)/2}$ obtained by bent functions concatenation) in 15 variables are in fact rotation symmetric. Moreover, Kavut et al. [25–27] proved that there exist rotation symmetric functions in 9 variables having nonlinearity 241 and 242 (which is also strictly greater than the bent concatenation nonlinearity $2^{9-1} - 2^{(9-1)/2}$), which was rather surprising and gives further motivation for the investigation of rotation symmetric Boolean functions.

Recently, there is some sustained effort to investigate the affine equivalence of some classes of Boolean functions, in particular the rotation symmetric Boolean functions (RSBF). In spite of their simplicity, the problem proves to be quite challenging. We mention here the papers [3,7,10–13] (and the references therein), which deal with low degrees (two to four) of

* Corresponding author.
E-mail addresses: dcanright@nps.edu (D. Canright), jong.chung@usma.edu (J.H. Chung), pstanica@nps.edu (P. Stănică).
[1] Current address: Department of Mathematical Sciences, United States Military Academy, West Point, NY 10996, USA.

http://dx.doi.org/10.1016/j.disc.2015.05.017
0012-365X/Published by Elsevier B.V.

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
2015		**00-00-2015 to 00-00-2015**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Circulant Matrices and Affine Equivalence of Monomial Rotation Symmetric Boolean Functions	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Naval Postgraduate School,Department of Applied Mathematics,Monterey,CA,93943**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The goal of this paper is two-fold. We first focus on the problem of deciding whether two monomial rotation symmetric (MRS) Boolean functions are affine equivalent via a permutation. Using a correspondence between such functions and circulant matrices, we give a simple necessary and sufficient condition. We connect this problem with the well known ??d??m???s conjecture from graph theory. As applications, we reprove easily several main results of Cusick et al. on the number of equivalence classes under permutations for MRS in prime power dimensions, as well as give a count for the number of classes in pq number of variables, where p, q are prime numbers with p < q < p2. Also, we find a connection between the generalized inverse of a circulant matrix and the invertibility of its generating polynomial over F2, modulo a product of cyclotomic polynomials, thus generalizing a known result on nonsingular circulant matrices.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**15**	

monomial RSBFs, or some particular cases of the dimension where the functions are defined. Here, we propose a more elegant (we believe) approach for equivalence, which works for any degree, and apply it to count some cubic equivalence classes.

Here is an outline of this work. Section 2 gives basic definitions, including monomial rotation symmetric (MRS) Boolean functions and affine equivalence, and a known result for such quadratic functions. Section 3 discusses computational complexity of determining affine equivalence. Section 4 gives several useful facts about circulant matrices. In Section 5, we define S-equivalence (affine-equivalent by permutation matrix) and show in detail the connection between MRS functions and circulant matrices, resulting in our Theorem 5.2 that S-equivalence of the functions is the same as P-Q equivalence of the matrices. In Section 6 we use this connection, along with a powerful result of Wiedemann and Zieve [40], to give new proofs for counting the number of equivalence classes for cubic MRS functions, in three cases: degree $n = p$ prime (our Theorem 6.3), $n = p^k$ prime power (Theorem 6.5), and $n = pq$ product of two primes (Theorem 6.6). In Section 7, we explore how a circulant matrix inverse, pseudoinverse, or generalized inverse might relate to function equivalence. First, Theorem 7.3 generalizes a previous result, to give a condition on the factors of the generating polynomial that guarantee the circulant matrix has a circulant reflexive generalized inverse. Then Theorem 7.8 gives a necessary condition on weights when functions are S-equivalent with invertible circulant matrices. Also, Theorem 7.12 gives some facts about the case when the matrix has a pseudoinverse.

2. Preliminaries

A Boolean function f on n variables may be viewed as a mapping from $\mathbb{F}_2^n = \{0, 1\}^n$ into the two-element field $\mathbb{F}_2$; it can also be interpreted as the output column of its *truth table* f, that is, a binary string of length 2^n, $f = [f(0, 0, \ldots, 0), f(1, 0, \ldots, 0), \ldots, f(1, 1, \ldots, 1)]$. The set of all Boolean functions is denoted by $\mathcal{B}_n$.

The addition operator over $\mathbb{F}_2$ is denoted by $+$. An n-variable Boolean function f can be considered to be a multivariate polynomial over $\mathbb{F}_2$. This polynomial can be expressed as a sum of products representation of all distinct kth order products $(0 \le k \le n)$ of the variables. More precisely, $f(x_1, \ldots, x_n)$ can be written as

$$a_0 + \bigoplus_{1\le i\le n} a_i x_i + \bigoplus_{1\le i<j\le n} a_{ij} x_i x_j + \cdots + a_{12\ldots n} x_1 x_2 \ldots x_n,$$

where the coefficients $a_0, a_{ij}, \ldots, a_{12\ldots n} \in \{0, 1\}$. This representation of f is called the *algebraic normal form* (ANF) of f. The number of variables in the highest order product term with nonzero coefficient is called the *algebraic degree*, or simply the degree of f and denoted by $deg(f)$. A Boolean function is said to be *homogeneous* if its ANF contains terms of the same degree only.

Functions of degree at most one are called *affine* functions. An affine function with constant term equal to zero is called a *linear* function. Let $\mathbf{x} = (x_1, \ldots, x_n)$ and $\boldsymbol{\omega} = (\omega_1, \ldots, \omega_n)$ both belong to $\mathbb{F}_2^n$ and $\mathbf{x}\cdot\omega = x_1\omega_1 + \cdots + x_n\omega_n$. The *Hamming distance* between $\mathbf{x}$ and ω, denoted by $d(\mathbf{x}, \boldsymbol{\omega})$, is the number of positions where $\mathbf{x}$, ω differ. Also the *(Hamming) weight*, denoted by $wt(\mathbf{x})$, of a binary string $\mathbf{x}$ is the number of ones in $\mathbf{x}$. An n-variable function f is said to be *balanced* if its output column in the truth table contains equal number of 0's and 1's (i.e., $wt(f) = 2^{n-1}$). The nonlinearity of an n-variable function f is the minimum distance to the entire set of all affine functions, distance known to be bounded from above by $2^{n-1} - 2^{n/2-1}$. We define the (right) rotation operator ρ_n on a vector $(x_1, x_2, \ldots, x_n) \in \mathbb{F}_2^n$ by $\rho_n(x_1, x_2, \ldots, x_n) = (x_n, x_1, x_2, \ldots, x_{n-1})$. Hence, ρ_n^k acts as a k-cyclic rotation on an n-bit vector. A Boolean function f is called *rotation symmetric* if for each input $(x_1, \ldots, x_n)$ in $\mathbb{F}_2^n$, $f(\rho_n^k(x_1, \ldots, x_n)) = f(x_1, \ldots, x_n)$, for $1 \le k \le n$. That is, the rotation symmetric Boolean functions are invariant under cyclic rotation of inputs. The inputs of a rotation symmetric Boolean function can be divided into partitions so that each partition consists of all cyclic shifts of one input. A partition is generated by $G_n(x_1, x_2, \ldots, x_n) = \{\rho_n^k(x_1, x_2, \ldots, x_n) | 1 \le k \le n\}$ and the number of sets in this partition is denoted by g_n. Thus the number of n-variable RSBFs is 2^{g_n}. Let $\phi(k)$ be Euler's *phi*-function, then Stănică and Maitra [37] give $g_n = \frac{1}{n}\sum_{k|n} \phi(k)\, 2^{\frac{n}{k}}$. We refer to [37,31,30] for the formula on how to calculate the number of partitions with weight w, for arbitrary n and w, as well as the number h_n of full length n classes (Ref. [28] corrects the count of [37] for h_n, when n is not a prime power).

A rotation symmetric function $f(x_1, \ldots, x_n)$ can be (for short) written as

$$a_0 + a_1 x_1 + \sum a_{1j} x_1 x_j + \cdots + a_{12\ldots n} x_1 x_2 \ldots x_n,$$

where the coefficients $a_0, a_1, a_{1j}, \ldots, a_{12\ldots n} \in \{0, 1\}$, and the existence of a representative term $x_1 x_{i_2} \ldots x_{i_l}$ implies the existence of all the terms from $G_n(x_1 x_{i_2} \ldots x_{i_l})$ in the ANF. This representation of f (not unique, since one can choose any representative in $G_n(x_1 x_{i_2} \ldots x_{i_l})$) is called the *short algebraic normal form* (SANF) of f. If the SANF of f contains only one term, we call such a function a *monomial rotation symmetric* (MRS) function. Certainly, the number of terms in the ANF of a monomial rotation symmetric function is a divisor of n (see [37]). If that divisor is in fact n, we call the function a *full-cycle MRS*, otherwise a *short-cycle MRS*.

We say that two Boolean functions $f(\mathbf{x})$ and $g(\mathbf{x})$ in $\mathcal{B}_n$ are *affine equivalent* if $g(\mathbf{x}) = f(\mathbf{x}A + \mathbf{b})$, where $A \in GL_n(\mathbb{F}_2)$ ($n \times n$ nonsingular matrices over the finite field $\mathbb{F}_2$ with the usual operations) and $\mathbf{b}$ is an n-vector over $\mathbb{F}_2$. We say $f(\mathbf{x}A + \mathbf{b})$ is a *nonsingular affine transformation* of $f(\mathbf{x})$. It is easy to see that if f and g are affine equivalent, then they have the same weight and nonlinearity: $wt(f) = wt(g)$ and $N_f = N_g$ (these are examples of *affine invariants*).

The relevance of these two invariants can be inferred by recalling the well-known result (see [10], for example).

Theorem 2.1. *Two quadratic functions f and g in $\mathcal{B}_n$ are affine equivalent if and only if $wt(f) = wt(g)$ and $N_f = N_g$.*

Unfortunately, the result (as stated) cannot be extended to higher degrees. In addition to our first approach for equivalence, in our second approach (a counterpart to the previous theorem) we obtain another criterion based on weight for degrees ≥ 2, which unfortunately, will turn out to be just necessary, but not sufficient. In spite of that, it can be used successfully to show non-equivalence in many cases.

3. Complexity comments

Besides the pure mathematical interest, affine equivalence is of major interest in cryptography. Two major methods in the study of S-boxes used in block ciphers, namely differential and linear cryptanalysis, are invariant under affine transformations. It is not only convenient, but also of vital importance to study only one representative of the affine equivalence class with respect to these attacks.

Moreover, even from an implementation point of view there may be other representations of the same cipher, with the same resistance against attacks, but using affine equivalent S-boxes, which are simpler to implement (in software and hardware). The simpler systems of low-degree equations obtained as a result of understanding the affine equivalence classes of S-boxes may be useful in designing countermeasure against some attacks, like the side-channel attacks [5,8].

A direct affine equivalence verification requires a search over all elements of $GL_n(\mathbb{F}_2)$, and this has computational complexity $O(2^{n^2})$, which becomes quite difficult for $n \geq 7$. Certainly, there are (simple) algebraic properties of Boolean functions, which are invariant under affine transformations, like the algebraic degree and the frequency distribution of the absolute values in the Walsh or autocorrelation spectrum (all of which were used in Fuller's Ph.D. thesis [20], for example), but these fail to *completely* distinguish affine equivalence. In fact, these criteria already fail for $n = 6$, as was pointed out in [21]. Two more complicated affine invariants were introduced in [6], but they also fail for $n > 6$.

Some version of these questions have been looked at, starting with Harrison's paper [22], and major advances have been made for small degrees ≤ 4, e.g. [7,10,11,14,12,13], but no major advances have been made for general high degree Boolean functions. Berlekamp and Welch [2] in 1972 found explicitly all equivalence classes for functions on 5 variables, and in 1991, Maiorana [29] looked at 6 variables and found 150, 357 such equivalence classes (both of these results also allowed transformations of the output).

We point out that two algorithms for checking affine equivalence have been proposed by Biryukov et al. [5] with time complexity $O(n^3 2^{2n})$, so they will work efficiently for small, say $n \leq 32$, dimensions. However, these algorithms fail to attack the general problem.

4. Circulant matrices and a group structure

We will concentrate on matrices whose entries are in the two-element field $\mathbb{F}_2$. An $n \times n$ matrix C is *circulant*, denoted by $C(c_1, c_2, \ldots, c_n)$, if all its rows are successive circular rotations of the first row, that is,

$$C = \begin{pmatrix} c_1 & c_2 & . & . & c_n \\ c_n & c_1 & . & . & c_{n-1} \\ . & . & . & . & . \\ c_2 & c_3 & . & . & c_1 \end{pmatrix}.$$

It is interesting to note the following equivalent way of defining circulant matrices, whose proof is immediate: an $n \times n$ matrix $C = \{c_{ij}\}$ is circulant if and only if $c_{ij} = c_{uv}$ whenever $j - i \equiv v - u \pmod n$. We further define the *generating polynomial* F of a circulant matrix $C(c_1, \ldots, c_n)$ by

$$F(z) = c_1 + c_2 z + \cdots + c_n z^{n-1}.$$

It is well-known (see, for instance, [18]) that the set $\mathcal{C}_n$ of all $n \times n$ circulant matrices forms a commutative algebra. Moreover, every matrix in $\mathcal{C}_n$ is normal; recall that a normal (real) matrix A is one which satisfies $A^T A = AA^T$, where A^T is the transpose of the matrix (actually, circulant matrices commute with each other, in general, as shown below in Lemma 4.1). Much more is known about circulant matrices C: for instance, their determinant can be expressed in terms of nth roots of unity, say ω, and C can be diagonalized via the Fourier matrix whose ith row is $(1, \omega^i, \omega^{2i}, \ldots, \omega^{(n-1)i})$. The interested reader can consult the myriad of research papers on circulant (and Toeplitz) matrices (e.g., [18]). However, some results on circulant complex matrices do not carry over to circulant matrices over a finite field, which makes their use a bit more complicated in that environment.

Below we display a result that will be proved to be quite useful. Let G be the $n \times n$ binary circulant matrix $G = C(0, 1, 0, \ldots, 0)$. Since for any $A = C(a_1, a_2, \ldots, a_n) \in \mathcal{C}_n$, then $A = \sum_{i=1}^{n} a_i G^{i-1} = \sum_{i \in \Delta(A)} G^{i-1}$, $a_i \in \mathbb{F}_2$, where $\Delta(A) \equiv \{i |\, a_i = 1\} \subseteq \{1, 2, \ldots, n\}$, and so, that the powers $\leq n - 1$ of G form a basis for the commutative algebra $\mathcal{C}_n$.

The next well-known lemma shows that the multiplication of circulant matrices is commutative.

Lemma 4.1. *Let $A = \mathrm{C}(a_1, a_2, \ldots, a_n)$ and $B = \mathrm{C}(b_1, b_2, \ldots, b_n)$ be two elements of $\mathcal{C}_n$. Then,*

$$AB = BA = \mathrm{C}\left(\sum_{\substack{i,j=1\\ i+j\equiv 2 \pmod n}}^{n} a_i b_j, \sum_{\substack{i,j=1\\ i+j\equiv 3 \pmod n}}^{n} a_i b_j, \ldots, \sum_{\substack{i,j=1\\ i+j\equiv 1 \pmod n}}^{n} a_i b_j\right)$$
$$= \mathrm{C}\left(\sum_{\substack{i\in\Delta(A), j\in\Delta(B)\\ i+j\equiv 2 \pmod n}} a_i b_j, \sum_{\substack{i\in\Delta(A), j\in\Delta(B)\\ i+j\equiv 3 \pmod n}} a_i b_j, \ldots, \sum_{\substack{i\in\Delta(A), j\in\Delta(B)\\ i+j\equiv 1 \pmod n}} a_i b_j\right).$$

Corollary 4.2. *Let $A = \mathrm{C}(a_1, a_2, \ldots, a_n)$ be a circulant matrix over $\mathbb{F}_2$. Then*

$$A^2 = \mathrm{C}\left(\sum_{\substack{i=1\\ 2i\equiv 2 \pmod n}}^{n} a_i, \sum_{\substack{i=1\\ 2i\equiv 3 \pmod n}}^{n} a_i, \ldots, \sum_{\substack{i=1\\ 2i\equiv 1 \pmod n}}^{n} a_i\right)$$
$$= \begin{cases} \mathrm{C}(a_1, a_{\lceil n/2\rceil+1}, a_2, a_{\lceil n/2\rceil+2}, \ldots) & \text{if } n \text{ is odd} \\ \mathrm{C}(a_1 + a_{n/2+1}, 0, a_2 + a_{n/2+2}, 0, \ldots) & \text{if } n \text{ is even.} \end{cases}$$

An $n \times n$ *permutation* matrix P_σ is an $n \times n$ matrix obtained by applying a permutation $\sigma \in S_n$ (the symmetric group) to the rows (or, equivalently, columns) of the identity matrix I_n.

We define a relation on the set of $n \times n$ circulant matrices as follows. Let $A_1 = \mathrm{C}(a_1, \ldots, a_n), A_2 = \mathrm{C}(b_1, \ldots, b_n)$. Then

$$A_1 \sim A_2 \text{ if and only if } (a_1, \ldots, a_n) = \rho_n^k(b_1, \ldots, b_n), \quad \text{for some } 0 \le k \le n-1.$$

It is immediate that the relation $\sim$ is an equivalence relation, which partitions $\mathcal{C}_n$ in equivalence classes, whose set will be denoted by $\mathcal{C}_n/_\sim$. We will denote the equivalence class of $\mathrm{C}(a_1, a_2, \ldots, a_n)$ by $\langle \mathrm{C}(a_1, a_2, \ldots, a_n)\rangle$.

Lemma 4.3. *For two arbitrary invertible circulant matrices M_1, M_2, then $M_1 \sim M_2$ if and only if $M_1^{-1} \sim M_2^{-1}$.*

Proof. Take $M_1 = \mathrm{C}(a_1, a_2, \ldots, a_n), M_2 = \mathrm{C}(b_1, b_2, \ldots, b_n)$ and $M_1^{-1} = \mathrm{C}(\alpha_1, \alpha_2, \ldots, \alpha_n)$ and $M_2^{-1} = \mathrm{C}(\beta_1, \beta_2 \ldots, \beta_n)$. It is sufficient to show that $M_2^{-1} \in \langle \mathrm{C}(\alpha_1, \alpha_2, \ldots, \alpha_n)\rangle$.

We know that $(b_1, b_2, \ldots, b_n) = \rho_n^k(a_1, a_2, \ldots, a_n)$ for some k. Thus, there is a circulant permutation matrix

$$P_k = \mathrm{C}(\rho_n^k(1, 0, \ldots, 0)) = G^k \quad \text{such that } M_2 = M_1 P_k$$

(where again G generates the standard basis for $n \times n$ circulant matrices). Taking inverses and using Lemma 4.1 gives

$$M_1^{-1} = P_k M_2^{-1} = M_2^{-1} P_k,$$

so $M_1^{-1} \sim M_2^{-1}$. Further, comparing first rows, where P_k rotates a row, we get $(\alpha_1, \ldots, \alpha_n) = \rho_n^k(\beta_1, \ldots, \beta_n)$, which shows the necessity of our claim. The sufficiency is immediate. □

Theorem 4.4. *The set $(\mathcal{C}_n/_\sim, \cdot)$ with the operation $\langle A\rangle \cdot \langle B\rangle := \langle AB\rangle$ is a commutative monoid. Moreover, the previous operation partitions the invertible circulant matrices $\mathcal{C}_n$ into equivalence classes, say $\mathcal{C}_n^*/_\sim$, and consequently, $(\mathcal{C}_n^*/_\sim, \cdot)$ becomes a group.*

Proof. First, we show that the operation is well-defined. Let $A = \mathrm{C}(a_1, \ldots, a_n) \sim A' = \mathrm{C}(a'_1, \ldots, a'_n), B = \mathrm{C}(b_1, \ldots, b_n) \sim B' = \mathrm{C}(b'_1, \ldots, b'_n)$. We need to show that $AB \sim A'B'$. Take k, s such that $\rho_n^k(a_1, \ldots, a_n) = (a'_1, \ldots, a'_n)$ and $\rho_n^s(b_1, \ldots, b_n) = (b'_1, \ldots, b'_n)$. That is, $A' = AG^k$, $B' = BG^s$. By Lemma 4.1,

$$A'B' = AG^k BG^s = ABG^{k+s} = ABG^{k+s \bmod n}$$

so $A'B' \sim AB$ (by $\rho_n^{k+s \bmod n}$).

The associative property then follows from that of matrix multiplication. The identity element is $\langle \mathrm{C}(1, 0, \ldots, 0)\rangle = \langle I_n\rangle$, the class of the identity matrix. The commutative property follows from the commutative property of the circulant matrices.

By Lemma 4.3, for nonsingular M we can let $\langle M\rangle^{-1}$ (which is well-defined) be the equivalence class of all inverses of circulant matrices from $\langle M\rangle$. Clearly, $\langle M\rangle \cdot \langle M\rangle^{-1} = \langle M\rangle \cdot \langle M^{-1}\rangle = \langle I_n\rangle$, and the result is shown. □

5. *S*-equivalence of monomial rotation symmetric Boolean functions

The goal in this section is to investigate the affine equivalence of monomial rotation symmetric (MRS) functions f, g under permutation of variables, which we call *S-equivalence* and denote by $f \overset{S}{\sim} g$. We will see that there is a strong connection between MRS functions and circulant matrices, which can help in determining the S-equivalence.

Example 5.1. Let $n = 7$, and the quartic MRS

$$f(\mathbf{x}) = x_1x_2x_3x_4 + x_2x_3x_4x_5 + x_3x_4x_5x_6 + x_4x_5x_6x_7 + x_5x_6x_7x_1 + x_6x_7x_1x_2 + x_7x_1x_2x_3,$$
$$g(\mathbf{x}) = x_1x_2x_4x_6 + x_2x_3x_5x_7 + x_3x_4x_6x_1 + x_4x_5x_7x_2 + x_5x_6x_1x_3 + x_6x_7x_2x_4 + x_7x_1x_3x_5.$$

Using the permutation $\pi = (2, 3, 5)(4, 7, 6)$ (product of disjoint cycles), one can check that $f \circ \pi = g$.

Let $f = x_1x_{j_2} \cdots x_{j_d} + x_2x_{j_2+1} \cdots x_{j_d+1} + \cdots + x_nx_{j_2-1} \cdots x_{j_d-1}$ be a MRS function of degree d, with the SANF $x_1x_{j_2} \cdots x_{j_d}$. We associate to f the following circulant matrix equivalence class

$$A_f = \langle C(\overset{1}{\underset{\downarrow}{1}}, 0, \ldots, \overset{j_2}{\underset{\downarrow}{1}}, 0, \ldots, 0, \overset{j_3}{\underset{\downarrow}{1}}, \ldots, 0, \overset{j_d}{\underset{\downarrow}{1}}, \ldots, 0)\rangle, \tag{1}$$

where the 1 bits (indicated above) appear in positions given by the indices in the SANF monomial of f. Of course, the SANF for f is not unique, but the equivalence class A_f is.

We extend the Δ notation for binary circulant matrices to a few other domains. For a binary (row) vector $(a_1, a_2, \ldots, a_n)$ of dimension n, let $\Delta(a_1, a_2, \ldots, a_n) \equiv \{i | a_i = 1\}$, so for a bit vector $\mathbf{a}$ the connection with the corresponding circulant matrix is clear: $\Delta(C(\mathbf{a})) = \Delta(\mathbf{a})$. Similarly, for a single monomial term $x_{i_1}x_{i_2} \cdots x_{i_d}$ of degree d in n variables, we define $\Delta(x_{i_1}x_{i_2} \cdots x_{i_d}) \equiv \{i_j | j = 1, 2, \ldots, d\}$. We can also extend this to the MRS function with this SANF, $f = x_{i_1}x_{i_2} \cdots x_{i_d}$, as $\Delta(f) = \Delta(x_{i_1}x_{i_2} \cdots x_{i_d})$; this is not unique, but for this usage we prefer to simply consider all such sets equal under a cyclic rotation permutation of the indices, so we will not unnecessarily complicate the notation. That is, for A_f as (1), then $\Delta(f) = \{1, j_2, \ldots, j_d\} = \{2, j_2 + 1, \ldots, j_d + 1\} = \cdots$. Then any particular set Δ of indices (out of n) defines: a unique monomial $x_{i_1}x_{i_2} \cdots x_{i_d}$ in n binary variables; a unique n-dimensional bit vector $\mathbf{a}$; the corresponding unique circulant matrix $C(\mathbf{a})$; the corresponding unique matrix equivalence class $\langle C(\mathbf{a})\rangle$; and the corresponding unique MRS function $f = x_{i_1}x_{i_2} \cdots x_{i_d}$ (SANF) such that $A_f = \langle C(\mathbf{a})\rangle$.

The details of the correspondence between f in n variables and A_f are as follows. The MRS f of degree d is the sum of k distinct monomials, where k divides n. Each monomial corresponds to a unique row vector (as above) where both have the same set of indices Δ; the degree d of the monomial is the weight of the vector and the size of the set. The equivalence class A_f comprises k distinct circulant matrices; their first rows correspond to the k monomials. For each matrix in A_f, the first k rows are distinct, and these rows repeat $r = n/k$ times. So each matrix has the same multi-set of rows as the others.

We now consider another type of equivalence between circulant matrices, which can be extended to the equivalence classes we have defined. For two circulant matrices A, B, if there are permutation matrices P, Q such that $PA = BQ$, then A and B are called P-Q equivalent. It is known in that case that AA^T and BB^T are similar matrices (in fact, there exists a permutation matrix which conjugates one to the other) [40]. Moreover, it is rather straightforward to see that $AA^T = \sum_{i,j\in\Delta(A)} G^{i-j}$, where $A = C(a_1, \ldots, a_n)$. This actually points to the importance of the differences $i - j$, which played a role in Cusick's paper [10], dealing with $wt(\Delta(f)) = 3$, only.

Note that since any two representative matrices A_1, A_2 of an equivalence class $\langle A\rangle$ are related by a rotation of the row order, there is a circulant permutation matrix R ($= G^k$ for some k) such that $A_1 = RA_2 = A_2R$. So the notion of P-Q equivalence extends naturally from circulant matrices to equivalence classes. That is, if $A_1 = R_AA_2$, $B_1 = B_2R_B$, and $P_1A_1 = B_1Q_1$, then $P_2A_2 = B_2Q_2$ where $P_2 = P_1R_A$ and $Q_2 = R_BQ_1$. In this sense, we can say that the classes $\langle A\rangle$, $\langle B\rangle$ are P-Q equivalent. For functions f, g where A_f and A_g are P-Q equivalent, it is customary to write $f \overset{P-Q}{\sim} g$.

The next result is not hard to show, but it provides a way to "move" the S-equivalence problem into the realm of matrix equivalences.

Theorem 5.2. *Two MRS Boolean functions f, g in n variables are S-equivalent if and only if their corresponding circulant matrix equivalence classes A_f and A_g are P-Q equivalent.*

Proof. Let A, B be representative circulant matrices of the classes A_f, A_g, respectively.

Assume f, g are S-equivalent. Then there is a permutation matrix Q that permutes the variables in the row vector $\mathbf{x}$ such that $f(\mathbf{x}Q) = g(\mathbf{x})$. Let $\mathbf{y} = \mathbf{x}Q$, so $f(\mathbf{y}) = g(\mathbf{x})$. From (1) we know that the column positions of the 1s in a row of B indicate which bit variables of $\mathbf{x}$ appear in the corresponding monomial term of g. Applying the permutation Q to each row thus permutes the column order to give BQ, in which the new column positions of the 1s in a row now indicate which bit variables of $\mathbf{y}$ appear in the corresponding monomial term of f, by S-equivalence. Hence, each of the rows in BQ appears in A. If g is full-cycle, each row is distinct, and f is full-cycle as well, and so we can reorder the rows with a permutation matrix P to get $PA = BQ$. Or if g has a short cycle of length k, then the first k rows of BQ repeat $r = n/k$ times, and f has the same cycle length and number of repetitions of rows in A, that is, both BQ and A have the same multi-set of rows. So again we can permute the rows to get $PA = BQ$.

Now assume that there are permutation matrices P, Q such that $PA = BQ$. Then the same reasoning applies in reverse: A and BQ have the same (multi-)set of rows, corresponding to the terms of f; each row in BQ applies the same permutation Q of bit variables to the corresponding terms of g. Thus $f(\mathbf{x}Q) = g(\mathbf{x})$, that is, f, g are S-equivalent. □

Example 5.3. Here we continue Example 5.1 of quartics for $n = 7$, with the same functions $f(\mathbf{x})$, $g(\mathbf{x})$ and permutation π where $f \circ \pi = g$. Applying π to the columns of an identity matrix gives a permutation matrix Q, that will permute the

column order of a vector $\mathbf{x}$ to that of $\mathbf{y} = \pi(\mathbf{x}) = \mathbf{x}Q$; so $f(\mathbf{y}) = g(\mathbf{x})$. Let A, B be circulant matrices corresponding to f, g, as shown below. Then for rows in BQ, the column order of $\mathbf{x}$ is permuted to that of $\mathbf{y}$, matching rows of A, but not in circulant order. So there is a row permutation matrix P such that $PA = BQ$ as shown below:

$$BQ = \begin{pmatrix} 1&1&0&1&0&1&0\\ 0&1&1&0&1&0&1\\ 1&0&1&1&0&1&0\\ 0&1&0&1&1&0&1\\ 1&0&1&0&1&1&0\\ 0&1&0&1&0&1&1\\ 1&0&1&0&1&0&1 \end{pmatrix} \begin{pmatrix} 1&0&0&0&0&0&0\\ 0&0&0&0&1&0&0\\ 0&1&0&0&0&0&0\\ 0&0&0&0&0&1&0\\ 0&0&1&0&0&0&0\\ 0&0&0&0&0&0&1\\ 0&0&0&1&0&0&0 \end{pmatrix} = \begin{pmatrix} 1&0&0&0&1&1&1\\ 0&1&1&1&1&0&0\\ 1&1&0&0&0&1&1\\ 0&0&1&1&1&1&0\\ 1&1&1&0&0&0&1\\ 0&0&0&1&1&1&1\\ 1&1&1&1&0&0&0 \end{pmatrix}$$

$$= PA = \begin{pmatrix} 0&0&0&0&1&0&0\\ 0&1&0&0&0&0&0\\ 0&0&0&0&0&1&0\\ 0&0&1&0&0&0&0\\ 0&0&0&0&0&0&1\\ 0&0&0&1&0&0&0\\ 1&0&0&0&0&0&0 \end{pmatrix} \begin{pmatrix} 1&1&1&1&0&0&0\\ 0&1&1&1&1&0&0\\ 0&0&1&1&1&1&0\\ 0&0&0&1&1&1&1\\ 1&0&0&0&1&1&1\\ 1&1&0&0&0&1&1\\ 1&1&1&0&0&0&1 \end{pmatrix}.$$

Note that certain symmetries may be applied to one equivalence class to get another equivalence class (or the same one again). One obvious symmetry preserved by rotation is reversal of a bit vector $\mathbf{x} = (x_1, x_2, \ldots, x_{n-1}, x_n)$, that is, $\mathbf{x}' = (x_n, x_{n-1}, \ldots, x_2, x_1)$. For example, for $n = 8$, if the cubic f has $\Delta(f) = \{1, 2, 4\}$, then applying reversal to everything in the equivalence class of f gives the equivalence class of g where $\Delta(g) = \{5, 7, 8\}$. Of course this is the same equivalence class, since bit reversal is an affine transformation. Another symmetry, which is not an affine transformation, is bitwise complementation. If we complement everything in the equivalence class of f, we get the equivalence class of the quintic h where $\Delta(h) = \{3, 5, 6, 7, 8\}$. In terms of matrices, if we let 1 represent the matrix of all 1's, then if $PA = BQ$ then $P(A+1) = PA+1 = BQ+1 = (B+1)Q$. So results on low-degree MRS polynomials apply to corresponding high-degree ones.

6. Counting cubic equivalence classes

We now give an application of our Theorem 5.2 that shows easily several theorems of Cusick [10, Theorem 4.2], Cusick and Brown [11]. We also show a result on dimension which is not a prime, nor a power of a prime (we learned meanwhile that this result is the subject of the new paper [14]).

Since it is going to be used throughout, we state the following theorem from Wiedemann and Zieve [40, Theorem 1.1] connecting the well-known Ádám conjecture from graph theory with our problem at hand.

Theorem 6.1. *Let A, B be two $n \times n$ 0/1-circulants of weight at most 3 with first rows support indices $\Delta(A)$, respectively, $\Delta(B)$. Then the following are equivalent:*

1. *There exist $u, v \in \mathbb{Z}_n$ such that $\gcd(u, n) = 1$ and $\Delta(A) = u\Delta(B) + v$.*
2. *A, B are P-Q equivalent.*
3. *There is an $n \times n$ permutation matrix P such that $AA^T = PBB^TP^{-1}$.*
4. *The complex matrices AA^T, BB^T are similar, that is, $AA^T = S^{-1}(BB^T)S$, for some invertible $n \times n$ matrix S.*

Since these problems are inherently tedious, we display below our action plan for counting the equivalence classes.

Action Plan. *Regardless of the degree (although, here we deal with cubic MRS only), we single out a few simple type (or types) of tuples that each equivalence class has as representatives (indices). Then, we count the number of inequivalent such type(s).*

We start with a simple lemma. Cusick [10, Lemma 4.3] assumes that n is prime, so our lemma is more general. If there exist $u, v \in \mathbb{Z}_n$ with $\gcd(u, n) = 1$ such that $u\Delta(f) + v = \Delta(g)$, we use the notation $\Delta(f) \sim \Delta(g)$. Throughout this paper we use the "capital mod" notation $a \bmod n$ to mean the unique integer $b \in \{1, 2, \ldots, n\}$ such that $b \equiv a \bmod n$. We also use the notation $p^s \parallel k$ to mean $p^s | k$ and $p^{s+1} \not| k$, that is, s is the p-adic valuation of k.

Lemma 6.2. *The S-equivalence class of any cubic MRS h with $\Delta(h) = \{1, i, j\}$ where either $\gcd(i-1, n) = 1$, or $\gcd(j-1, n) = 1$, or $\gcd(i-j, n) = 1$, contains a function g with $\Delta(g) = \{1, 2, m\}$. If $n = p^k$, $k \geq 2$, where p is a prime and $\gcd(i-1, n) \neq 1$, $\gcd(j-1, n) \neq 1$, then the class of h will not contain any MRS function g with $\Delta(g) = \{1, 2, \ell\}$, but it will contain an MRS g with $\Delta(g) = \{1, p^s + 1, m\}$, where $p^s \parallel \gcd(i-1, j-1)$, $1 \leq s \leq k-1$, and $p^s | (m-1)$.*

Proof. We first assume that at least one of $\gcd(i-1, n) = 1$, or $\gcd(j-1, n) = 1$, or $\gcd(i-j, n) = 1$. By Theorem 5.2 and [40, Theorem 1.1] it will be sufficient to show that for every MRS h with $\Delta(h) = \{1, i, j\}$, there exist u, v such that $u\Delta(h) + v = \{1, 2, m\}$, for some m. That is easily seen: if $\gcd(i-1, n) = 1$ take $u = (i-1)^{-1} \bmod n$, $v = 1 - u \bmod n$, $m = 1 + (j-1)u \bmod n$; or if $\gcd(j-1, n) = 1$ take $u = (j-1)^{-1} \bmod n$, $v = 1 - u \bmod n$, $m = 1 + (i-1)u \bmod n$; or if $\gcd(i-j, n) = 1$ take $u = (i-j)^{-1} \bmod n$, $v = 1 - ju \bmod n$, $m = 1 + (1-j)u \bmod n$.

Next assume that $1 \le s$ and $p^s \parallel \gcd(i-1, j-1)$ (and consequently, $p^s | (j-i)$). Without loss of generality, we assume that $p^s \parallel i-1$, and so $i-1 = p^s t$ for some $t \not\equiv 0 \pmod p$ (the other cases are similar). By taking $u = t^{-1} \bmod p$, $v = 1-u$, $m = 1+(j-1)u$, then we see that $\{1, i, j\} \sim \{1, p^s+1, m\}$ (and certainly $p^s | m-1 = (j-1)t^{-1}$, since $p^s \lfloor j-1$). □

For the following theorem, due to Cusick [10, Theorem 4.2], we can use Lemma 6.2 to give a simpler proof.

Theorem 6.3. *Suppose $p \ge 3$ is a prime. Then the number of S-equivalence classes of cubic MRS in p variables is*

$$E(p) = \left\lceil \frac{p}{6} \right\rceil.$$

Proof. We take $k = \lfloor p/6 \rfloor$, so $p = 6k+1$, or $p = 6k+5$. Also, a simple computer program reveals that the formula is correct for $p = 3, 5, 7$, so we will assume in what follows that $p \ge 11$. By our Theorem 5.2, two cubic MRS in n variables are equivalent if and only if the corresponding circulant matrices are P-Q equivalent. By Theorem 6.1 that happens if and only if there exist $u, v \in \mathbb{Z}_n$ with $\gcd(u, n) = 1$ such that $u\Delta(f) + v = \Delta(g)$ (recall the notation $\Delta(f) \sim \Delta(g)$). In this proof, not to introduce a new notation, we will use $\Delta(\cdot)$ for a representation of that support class.

Using Lemma 6.2, it will be sufficient to count the number of MRS f with $\Delta(f) = \{1, 2, m\}$, $m \ge 3$, that are not equivalent. We will look at the number of possible MRS g with $\Delta(g) = \{1, 2, \ell\}$ contained in the class of some MRS f with $\Delta(f) = \{1, 2, m\}$. Since there are $p-2$ choices for m, the result will follow by simple summation.

For $u, v \in \mathbb{Z}_p$, $u \ne 0$, if $u\Delta(f) + v = u\{1, 2, m\} + v = \Delta(g) = \{1, 2, \ell\}$, then we have several possibilities. As before, we adopt the convention that all expressions are $\bmod p$.

Case 1. $u + v = 1, 2u + v = 2, mu + v = \ell$. We obtain the solutions $(u, v, \ell) = (1, 0, m)$.

Case 2. $u + v = 1, 2u + v = \ell, mu + v = 2$. We obtain the solutions $(u, v, \ell) = \left((m-1)^{-1}, 1-(m-1)^{-1}, 1+(m-1)^{-1}\right)$.

Case 3. $2u + v = 1, u + v = 2, mu + v = \ell$. We obtain the solutions $(u, v, \ell) = (p-1, 3, 3-m)$.

Case 4. $2u + v = 1, u + v = \ell, mu + v = 2$. We obtain the solutions $(u, v, \ell) = \left((m-2)^{-1}, 1-2(m-2)^{-1}, 1-(m-2)^{-1}\right)$.

Case 5. $mu + v = 1, u + v = 2, 2u + v = \ell$. We obtain the solutions $(u, v, \ell) = \left(-(m-1)^{-1}, 2+(m-1)^{-1}, 2-(m-1)^{-1}\right)$.

Case 6. $mu + v = 1, u + v = \ell, 2u + v = 2$. We obtain the solutions $(u, v, \ell) = \left(-(m-2)^{-1}, 2+2(m-2)^{-1}, 2+(m-2)^{-1}\right)$.

Potentially, for every $3 \le m \le p$, there are 5 other possible MRS g with $\Delta(g) = \{1, 2, \ell\}$ in the same class as f with $\Delta(f) = \{1, 2, m\}$. However, not all of those values are different. So, let us look at the putative ℓ's in the set (all expressions are $\bmod p$):

$$\{m, 1+(m-1)^{-1}, 3-m, 1-(m-2)^{-1}, 2-(m-1)^{-1}, 2+(m-2)^{-1}\}. \tag{2}$$

If $m = 3$, then we easily see that $\ell \in \{3, 1+2^{-1}, p, p, 2-2^{-1}, 3\} = \{3, 1+2^{-1}, p\}$ (we use $1+2^{-1} \equiv 2-2^{-1} \bmod p$), that is, $\{1, 2, 3\} \sim \{1, 2, 1+2^{-1}\} \sim \{1, 2, p\}$. Assume now that $m \notin \{3, 1+2^{-1}, p\}$ (certainly, $1+2^{-1} \ne 3$, nor $p \bmod p$). Further, if $p \equiv 1 \pmod 6$, then Gauss' quadratic reciprocity law for the Jacobi symbol implies $(-1)^{(3-1)(p-1)/4} = (-1)^{3k} = \left(\frac{3}{p}\right)\left(\frac{p}{3}\right) = \left(\frac{3}{p}\right)\left(\frac{1}{3}\right) = \left(\frac{3}{p}\right)$ and $\left(\frac{-1}{p}\right) = (-1)^{3k}$, and so, -3 is a quadratic residue modulo p. Thus $(3 \pm (-3)^{1/2})2^{-1}$ exists $\bmod p$ (this is obtained by equating $m = 1-(m-2)^{-1} = 2-(m-1)^{-1}$, or $1+(m-1)^{-1} = 3-m = 2+(m-2)^{-1}$). If m is any of these two values $(3 \pm (-3)^{1/2})2^{-1}$, then the set (2) consists of only two elements. In all other cases, the set (2) contains six different elements, as one can easily see. Then the number of nonequivalent classes if $p \equiv 1 \pmod 6$ is

$$E(p) = 1 + 1 + \frac{p-2-5}{6} = \frac{6k+1+12-7}{6} = k+1.$$

If $p \equiv 5 \pmod 6$, then -3 is not a quadratic residue modulo p, and so, the above class of cardinality 2 does not exist. Thus, besides $\{3, 1+2^{-1}, p\}$, every other class contains six elements, and so, the number of equivalent classes for $p \equiv 5 \pmod 6$ is exactly

$$E(p) = 1 + \frac{p-2-3}{6} = \frac{6k+5+6-5}{6} = k+1.$$

Regardless, $E(p) = \left\lceil \frac{p}{6} \right\rceil$, and the proof is done. □

Next, we apply our method to show the main result of [11, Theorem 6.1]. We adopt the convention that working in some $\mathbb{Z}_n$, $x^{-1}p^t$ exists if $p^\alpha \parallel x = p^\alpha y$, $\alpha \le t$, and $p^t x^{-1} := p^{t-\alpha} y^{-1}$. We denote by $E(p^k)_1$, $E(p^k)_5$ the number of distinct equivalence classes of cubic MRS in p^k variables, for $p \equiv 1 \pmod 6$, respectively, $p \equiv 5 \pmod 6$. We start with a lemma.

Lemma 6.4. *Using the notations of Lemma 6.2, any class $\{1, p^s+1, ap^{s+1}+1\}$ (potentially, p could further divide a) is equivalent to a class $\{1, p^s+1, bp^s+1\}$, where $\gcd(b, p) = 1$. Furthermore, if $2 \le a$, $ap^s + 1 \le p^k$, $p^w < cp^w < p^k$ and $\{1, p^s+1, bp^s+1\} \sim \{1, p^w+1, cp^w+1\}$, $\gcd(bc, p) = 1$, then $s = w$. (All equivalences are considered $\bmod p^k$.)*

Proof. The first claim follows easily by taking, for instance, $u = -1$, $v = p^s + 2$, $b = 1 - ap$, since then $u\{1, p^s + 1, ap^{s+1} + 1\} + v = \{1, p^s + 1, bp^s + 1\}$.

Regarding the second claim, without loss of generality, we assume $0 \le s \le w$. Let u, v with $\gcd(u, p^k) = 1$ which maps the first onto the second support. Solving the corresponding systems we obtain the following possibilities for (u, v, c):

$$(P_1): \ \left(p^{w-s}, 1 - p^{w-s}, b\right);$$
$$(P_2): \ \left(p^{w-s}b^{-1}, 1 - p^{w-s}b^{-1}, b^{-1}\right);$$
$$(P_3): \ \left(-p^{w-s}, 1 + p^w + p^{w-s}, 1 - b\right);$$
$$(P_4): \ \left(p^{w-s}(b-1)^{-1}, 1 - p^{w-s}(p^s + 1)(b-1)^{-1}, -(b-1)^{-1}\right);$$
$$(P_5): \ \left(-p^{w-s}b^{-1}, 1 + p^w + p^{w-s}b^{-1}, 1 - b^{-1}\right);$$
$$(P_6): \ \left(-p^{w-s}(b-1)^{-1}, 1 + p^{w-s}(bp^s + 1)(b-1)^{-1}, b(b-1)^{-1}\right).$$

Certainly, (P_1) cannot happen unless $w = s$; in (P_2), since $c = b^{-1}$ and $p \not| b$, then $u = p^{w-s}b^{-1}$ and $\gcd(u, p) = 1$ forces $w = s$; in (P_3), since $u = -p^{w-s}$ and $\gcd(u, p) = 1$, we need $w = s$; in (P_4), since $c = -(b-1)^{-1}$, then $p \not| b - 1$, and so $u = p^{w-s}(b-1)^{-1}$ and $p \not| u$ forces $w = s$; in (P_5), since $p \not| b$, then $u = -p^{w-s}b^{-1}$ forces $w = s$; in (P_6), since $c = b(b-1)^{-1}$, then $p \not| b - 1$, and so $u = -p^{w-s}(b-1)^{-1}$ forces $w = s$. □

Theorem 6.5. *Let $p \ge 5$ be a prime number. The number of equivalence classes in p^k ($k \ge 2$) variables is*

$$E(p^k)_1 = \frac{(p+1)(p^k-1)}{6(p-1)} + \frac{2k}{3} \tag{3}$$

$$E(p^k)_5 = \frac{(p+1)(p^k-1)}{6(p-1)}. \tag{4}$$

Proof. Let h be a p^k ($k \ge 2$) variables cubic MRS with $\Delta(h) = \{1, i, j\}$. We first assume that $\gcd(i-1, n) = \gcd(j-1, n) = \gcd(i-j, n) = 1$. By Lemma 6.2, in the equivalence class of h there exist functions f with $\Delta(f) = \{1, 2, m\}$. As in Theorem 6.3, the only possibilities for ℓ with $\{1, 2, m\} \sim \{1, 2, \ell\}$ are in the set

$$\{m, 1 + (m-1)^{-1}, 3 - m, 1 - (m-2)^{-1}, 2 - (m-1)^{-1}, 2 + (m-2)^{-1}\}. \tag{5}$$

We distinguish several cases. We adopt the convention that the expressions are regarded Mod p^k.

Case 1. $\gcd(m-1, p) = \gcd(m-2, p) = 1$. As before, if $m = 3$, then the class of $\{1, 2, 3\}$ contains three distinct cases $\{1, 2, \ell\}$, where $\ell \in \{3, 1 + 2^{-1}, p^k\}$. As before, -3 is a quadratic residue modulo p^k when $p \equiv 1 \pmod 6$, and so, there is another class containing two functions g with $\Delta(g) = \{1, 2, (3 \pm (-3)^{1/2})2^{-1}\}$ in this case, only. Under the assumption $\gcd(m-1, p) = \gcd(m-2, p) = 1$ and $m \notin \{3, 1+2^{-1}, (3 \pm (-3)^{1/2})2^{-1}, p^k\}$, then the set (5) contains distinct elements.

Since $3 \le m \le p^k$, there are $p^k - 2$ choices for m, from which we take away the ones that do not satisfy $\gcd(m-1, p) = \gcd(m-2, p) = 1$ (there are $2(p^{k-1} - 1)$ of those), and so the contribution to $E(p^k)_1$ in this case is

$$1 + 1 + \frac{p^k - 2 - 2(p^{k-1} - 1) - 5}{6} = \frac{p^k - 2p^{k-1} + 7}{6}, \tag{6}$$

and to $E(p^k)_5$ is

$$1 + \frac{p^k - 2 - 2(p^{k-1} - 1) - 3}{6} = \frac{p^k - 2p^{k-1} + 3}{6}, \tag{7}$$

Case 2. $\gcd(m-1, p) \ne 1$, or $\gcd(m-2, p) \ne 1$ (obviously, they cannot both happen). Then there are four possible values for ℓ, namely $\ell \in \{m, 3-m, 1-(m-2)^{-1}, 2+(m-2)^{-1}\}$, if $\gcd(m-1, p) \ne 1$; or $\{m, 1+(m-1)^{-1}, 3-m, 2-(m-1)^{-1}\}$, if $\gcd(m-2, p) \ne 1$. (We observe that if $k = 2$, then either set can be simplified as $\{m, 3 - m, m + 1, 2 - m\}$, all distinct.)

The contribution to both $E(p^k)_1$ and $E(p^k)_5$ in this case is

$$\frac{2(p^{k-1} - 1)}{4} = \frac{p^{k-1} - 1}{2}. \tag{8}$$

We now look at the cases when the equivalence classes do not contain any MRS f with $\Delta(f) = \{1, 2, m\}$, rather $\{1, p^s + 1, m\}$ with $p^s | m - 1$, $1 \le s \le k - 1$.

Next, we fix s with $1 \le s \le k - 1$, and (by Lemma 6.4) we assume that the MRS classes based on $\{1, p^s + 1, ap^s + 1\}$ and $\{1, p^s + 1, bp^s + 1\}$ are equivalent, $2 \le a, b \le p^{k-s-1} - 1$, $\gcd(ab, p) = 1$. As before, using Theorem 6.1, the possible values

for $(b; u, v)$ such that $u\{1, p^s+1, ap^s+1\}+v = \{1, p^s+1, bp^s+1\}$ are:

$$\begin{aligned}&(a; 1, 0),\ (a^{-1}; a^{-1}, 1-a^{-1}),\ (1-a; -1, 2+p^s),\\ &((1-a)^{-1}; -(1-a)^{-1}, (2-a+p^s)(1-a)^{-1}),\\ &(1-a^{-1}; -a^{-1}, 1+p^s+a^{-1}),\\ &(1+(a-1)^{-1}; -(a-1)^{-1}, a(p^s+1)(a-1)^{-1}).\end{aligned} \tag{9}$$

Case 3. Let $a \not\equiv 0, 1 \pmod p$. If $a = 2$, then (9) (since it is not relevant for our discussion we give up the values of u, v) shrinks to

$$2, 2^{-1}, -1.$$

If $p \equiv 1 \pmod 6$, -3 is a quadratic residue modulo p^k, then for $a = (1 \pm (-3)^{1/2})2^{-1}$, the set of b's from (9) shrinks further into the set of cardinality two (since in this case $a = (1-a)^{-1} = 1-a^{-1}$ and $a^{-1} = 1-a = a(a-1)^{-1}$)

$$a, a^{-1}.$$

In this case, if $a \notin \{2, 2^{-1}, -1, (1\pm(-3)^{1/2})2^{-1}\}$ when $p \equiv 1 \pmod 6$, respectively, $a \notin \{2, 2^{-1}, -1\}$ when $p \equiv 5 \pmod 6$, then the set (9) contains six distinct elements.

The number of a's in the interval $[2, p^{k-s}-1]$ that are $\equiv 1 \pmod p$ is $(p^{k-s-1}-1)$, and so, the number of $a \not\equiv 0, 1 \pmod p$ is $(p^{k-s}-2)-2(p^{k-s-1}-1) = p^{k-s}-2p^{k-s-1}$. The contribution to $E(p^k)_1$ in this case (for every value of $1 \le s \le k-1$) is

$$\sum_{s=1}^{k-1}\left(1+1+\frac{(p^{k-s}-2p^{k-s-1})-5}{6}\right) = \frac{(p-2)p^{k-1}+p(7k-8)-7k+9}{6(p-1)} \tag{10}$$

and the contribution to $E(p^k)_5$ in this case (for every value of $1 \le s \le k-1$) is

$$\sum_{s=1}^{k-1}\left(1+\frac{(p^{k-s}-2p^{k-s-1})-3}{6}\right) = \frac{(p-2)p^{k-1}+p(3k-4)-3k+5}{6(p-1)}. \tag{11}$$

Case 4. Let $a \equiv 1 \pmod p$. Recall that $a \not\equiv 0 \pmod p$, so the only possibilities for b in (9) are

$$a, a^{-1}.$$

The contribution to $E(p^k)_1$, or $E(p^k)_5$ in this case (for every value of $1 \le s \le k-1$) is

$$\sum_{s=1}^{k-1}\frac{p^{k-s-1}-1}{2} = \frac{p^{k-1}-p(k-1)+k-2}{2(p-1)}. \tag{12}$$

Summing Eqs. (6), (8), (10), (12), respectively, with (7), (8), (11), (12), we obtain the expressions for $E(p^k)_1$, respectively, $E(p^k)_5$. □

To show that the number of cubic MRS in 2^k ($k \ge 4$) number of variables is $E(2^k) = 2^{k-1}+k-1$ is actually easier than the previous proof. We omit the details, but each class has as a representative either $\{1, 2, 3\}$, $\{1, 2, 2^{k-1}\}$, $\{1, 2, 2^{k-1}+1\}$ all of cardinality two, or some other $\{1, 2, m\}$ of cardinality four, or a triple $\{1, 2^s+1, a2^t+1\}$ of cardinality 1, 2, 4.

We independently derived the next result (we found out after submitting this work that the recent paper [14] gives this result with no restriction on p, q) that seemed complicated to obtain via the previously published methods, that is, we find the number of equivalence classes for cubic MRS in $n = pq$ (for primes $3 \le p < q$) variables.

Theorem 6.6. *Let $5 \le p < q < p^2$ be prime numbers. The number of S-equivalence classes for cubic MRS in $n = pq$ number of variables is*

$$\begin{aligned}E(pq)_{1,1} &= \frac{pq+2(p+q)+25}{6} \quad \text{if } p \equiv 1 \pmod 6, \text{ and } q \equiv 1 \pmod 6,\\ E(pq)_{1,5} &= \frac{pq+2(p+q)+13}{6} \quad \text{if } p \equiv 1 \pmod 6, \text{ and } q \equiv 5 \pmod 6,\\ E(pq)_{5,1} &= \frac{pq+2(p+q)+13}{6} \quad \text{if } p \equiv 5 \pmod 6, \text{ and } q \equiv 1 \pmod 6,\\ E(pq)_{5,5} &= \frac{pq+2(p+q)+9}{6} \quad \text{if } p \equiv 5 \pmod 6, \text{ and } q \equiv 5 \pmod 6.\end{aligned}$$

Proof. Let $\{1, i, j\}$ (with $1 < i < j$) be the support of an MRS. By Lemma 6.2, if $\gcd(i-1, n) = 1$, or $\gcd(j-1, n) = 1$, then its class will contain an MRS with support $\{1, 2, m\}$. Assume now that $\gcd(i-1, n) \ne 1$ and $\gcd(j-1, n) \ne 1$. There are

several options: either $p|\gcd(i-1, j-1)$, or $q|\gcd(i-1, j-1)$. As before it is easy to show that every such S-equivalent class will contain an MRS with support $\{1, p+1, ap+1\}$, $p \parallel \gcd(i-1, j-1)$, $a > 1$, respectively, $\{1, q+1, bq+1\}$, $q \parallel \gcd(i-1, j-1)$, $b > 1$, $\gcd(ab, pq) = 1$. Further, the classes $\{1, p+1, ap+1\}$ and $\{1, q+1, bq+1\}$ will never overlap, since otherwise, there exist $u, v \in \mathbb{Z}_{pq}$ with $\gcd(u, pq) = 1$ such that $u\{1, p+1, ap+1\} + v = \{1, q+1, bq+1\}$, which could only happen for (u, v, b) equal to one of the following six cases:

$$(qp, 1-qp, a);$$
$$\left(q(ap)^{-1}, 1-q(ap)^{-1}, a^{-1}\right);$$
$$\left(-qp^{-1}, 1+q+qp^{-1}, 1-a\right);$$
$$\left(q((a-1)p)^{-1}, 1+q(p+1)((1-a)p)^{-1}, (1-a)^{-1}\right);$$
$$\left(-q(ap)^{-1}, 1+q+q(ap)^{-1}, 1-a^{-1}\right);$$
$$\left(q((1-a)p)^{-1}, 1+q(ap+1)((a-1)p)^{-1}, a(a-1)^{-1}\right),$$

which are all impossible (since x is invertible if and only if $\gcd(x, pq) = 1$).

Thus, it is sufficient to count the disjoint classes containing $\{1, 2, m\}$, $\{1, p+1, ap+1\}$, or $\{1, q+1, bq+1\}$, with $\gcd(a, p) = 1$ and $gcd(b, q) = 1$.

Case 1. S-equivalent classes with a representative $\{1, 2, m\}$. If $\{1, 2, m\} \sim \{1, 2, \ell\}$, then the possible values for ℓ's are in the set:

$$\{m, 3-m, 1+(m-1)^{-1}, 1-(m-2)^{-1}, 2-(m-1)^{-1}, 2+(m-2)^{-1}\}. \tag{13}$$

Case 1.1. Let m be such that $p|m-1$, $q|m-2$, or $p|m-2$, $q|m-1$. Since in that case we need to have $ap - bq = 1$, it is known that there are two solutions for that identity with $|a| < q$, $|b| < p$ (if $a > 0$, $b > 0$, then the other values are $a' = a - q$, $b' = b - p$, and if $a < 0$, $b < 0$, then the other values are $a' = q + a$, $b' = p + b$), and therefore, two such values for m, say m_0, m_1 (if, for example, $m_0 = ap + 1 = bq + 2$, for some a, b, then $m_1 = (q-a)p + 2 = (p-b)q + 1$, all in Mod pq). Then $\{1, 2, m_0\} \sim \{1, 2, m_1\}$ (that is easily seen, since, for instance, if $m_0 = ap + 1 = bq + 2$, then by taking $(u, v, \ell) = (-1, 3, 2-ap) = (-1, 3, m_1)$, and we get the equivalence). (As an observation, these two values in (13) are $\{m, 3-m\}$.) Let m be such that $p|m-1$, $q|m-3$, or $p|m-3$, $q|m-1$. Then we need to have $\alpha p - \beta q = 2$, which is treated by the previous argument (in this case α, β are obtained by multiplying by 2 the previous pair a, b).

The contribution of this case to any of the $E(pq)_{\cdot,\cdot}$'s is

$$2. \tag{14}$$

Case 1.2. If $m = 3$, then we see that the class of $\{1, 2, 3\}$ contains $\{1, 2, m\}$, where $m \in \{3, 1+2^{-1}, pq\}$. If both $p, q \equiv 1 \pmod 6$, then -3 is a quadratic residue modulo pq and so, there are two more classes $\{1, 2, m\}$ of cardinality two, where $m = (3 \pm \alpha)2^{-1}$ Mod pq, with $\alpha^2 = -3 \pmod{pq}$ (recall that there are two values of $|\alpha|$).

The contribution of this case to both $E(pq)_{1,\cdot}$ and $E(pq)_{\cdot,1}$, respectively, $E(pq)_{5,5}$ is

$$1 + 2, \text{ respectively,} \tag{15}$$
$$1. \tag{16}$$

We next assume that $m \notin \{3, 1+2^{-1}, pq, (3 \pm (-3)^{1/2})2^{-1}\}$, if both $p, q \equiv 1 \pmod 6$ and that $m \notin \{3, 1+2^{-1}, pq\}$, if either $p, q \equiv 5 \pmod 6$.

Case 1.3. Let $\gcd(m-1, pq) \neq 1$, $\gcd(m-2, pq) = 1$, $\gcd(m-3, pq) = 1$, or $\gcd(m-1, pq) = 1$, $\gcd(m-2, pq) \neq 1$, $\gcd(m-3, pq) = 1$. The possible values of ℓ in this case, from Eq. (13), are

$$\{m, 3-m, 1-(m-2)^{-1}, 2+(m-2)^{-1}\}, \text{ respectively,}$$
$$\{m, 3-m, 1+(m-1)^{-1}, 2-(m-1)^{-1}\}.$$

It is easy to see that in reality the two possibilities will not have different contributions to $E(pq)_{\cdot,\cdot}$, since if $r|m-1$, for $r \in \{p, q\}$, then $r|(3-m)-2$. Thus, the number of m's in the interval $[3, pq]$, under the given conditions, is exactly $2(p+q-6)$, and so, the contribution of this case to $E(pq)_{\cdot,\cdot}$ is

$$\frac{2(p+q-6)}{4} = \frac{p+q-6}{2}. \tag{17}$$

We remark that we do not have to consider the case of $\gcd(m-1, pq) \neq 1$, $\gcd(m-2, pq) = 1$, $\gcd(m-3, pq) \neq 1$, or, $\gcd(m-1, pq) = 1$, $\gcd(m-2, pq) \neq 1$, $\gcd(m-3, pq) \neq 1$, since this prompts $\ell \in \{m, 3-m\}$, which was treated in Case 1.2.

By using an inclusion–exclusion argument, we see that the number of integers m with $\gcd(m-1, pq) \neq 1$ or $\gcd(m-2, pq) \neq 1$ is $2(p+q-3)$, and so, the contribution to $E(pq)_{1,1}$ of classes with representative $\{1, 2, m\}$ for this case is

$$2 + 1 + 2 + \frac{p+q-6}{2} + \frac{(pq-2) - 2(p+q-6) - 7}{6} = \frac{pq+p+q+15}{6}, \tag{18}$$

and the contribution to $E(pq)_{\cdot,5}$ or $E(pq)_{5,\cdot}$ is

$$2+1+\frac{p+q-6}{2}+\frac{(pq-2)-2(p+q-6)-3}{6}=\frac{pq+p+q+7}{6}. \tag{19}$$

Case 2. S-equivalent classes with a representative $\{1, p+1, ap+1\}$, where $2 \le a < p$, $\gcd(a, pq) = 1$. The possible values of a's are:

$$\{a, a^{-1}, 1-a, (a-1)^{-1}, 1-a^{-1}, 1+(a-1)^{-1}\}.$$

The set of possible a's for the equivalence class of $\{1, p+1, ap+1\}$ (using only the a's that satisfy $p+1 < ap+1 \le pq$, $\gcd(a, pq) = 1$) is $\{2, 2^{-1}, -1\}$ for $a = 2$; $\{(1 \pm \alpha)2^{-1} \bmod q\}$, $\alpha^2 \equiv -3 \pmod q$, if $q \equiv 1 \pmod 6$; or $\{a, a^{-1}, 1-a, (a-1)^{-1}, 1-a^{-1}, 1+(a-1)^{-1}\}$ in any other case. The contribution of this case to $E(pq)_{1,1}$ or $E(pq)_{5,1}$ is

$$1+1+\frac{(q-2)-3-2}{6}=\frac{q+5}{6} \tag{20}$$

and the contribution of this case to $E(pq)_{1,5}$ or $E(pq)_{5,5}$ is

$$1+\frac{(q-2)-3}{6}=\frac{q+1}{6}. \tag{21}$$

Case 3. S-equivalent classes with a representative $\{1, q+1, bq+1\}$, $2 \le b \le p-1$. The possible b's are:

$$\{b, b^{-1}, 1-b, (b-1)^{-1}, 1-b^{-1}, 1+(b-1)^{-1}\}. \tag{22}$$

Since $n = pq$, $p < q$, and $bq+1 < pq$, then $\gcd(b, pq) = \gcd(b-1, pq) = 1$. As before, there are two classes generated by $b \in \{2, 2^{-1}, -1\}$; or $b \in \{(1 \pm \beta)2^{-1} \bmod p\}$ ($\beta^2 \equiv -3 \pmod p$ if $p \equiv 1 \pmod 6$). If b is not any of these values, then the previous displayed set (22) has cardinality six. The contribution to $E(pq)_{1,\cdot}$ is

$$1+1+\frac{(p-2)-5}{6}=\frac{p+5}{6} \tag{23}$$

and the contribution of these cases to $E(pq)_{5,\cdot}$ is

$$1+\frac{(p-2)-3}{6}=\frac{p+1}{6}. \tag{24}$$

Thus, putting together Eqs. (18), (19), (20), (21), (23) and (24) we get the claim. □

Remark 6.7. If we do not impose the condition that $q < p^2$, then the only difference would be in Case 2, where we might have classes with representatives $\{1, p^s+1, ap^s+1\}$, $\gcd(a, pq) = 1$, where a could be:

$$\begin{aligned}
&\{a, a^{-1}\}, \quad \text{if } a \equiv 1 \pmod p;\\
&\{2, 2^{-1}, -1\}, \quad \text{for } a = 2;\\
&\{(1 \pm \alpha)2^{-1} \bmod q\}, \quad \alpha^2 \equiv -3 \pmod q, \quad \text{if } q \equiv 1 \pmod 6;\\
&\{a, a^{-1}, 1-a, (a-1)^{-1}, 1-a^{-1}, 1+(a-1)^{-1}\}, \quad \text{otherwise.}
\end{aligned}$$

Can our method based upon Theorem 5.2 and a result similar to Theorem 6.1 be extended to count the equivalence classes of quartic, quintic, etc., MRS? Presumably, yes, as long as the P-Q equivalence can be characterized via the equivalent residue classes, that is, $\Delta(f) \sim \Delta(g)$ where $\Delta(g) = u\Delta(f) + v$, $u, v \in \mathbb{Z}_n$, $\gcd(u, n) = 1$. For example, from what it is known [40] we infer that such a result happens for quartics, quintics in n variables, assuming that every prime factor of ℓ is greater than 23, respectively 40. We can also infer from what it is also known about Ádám's conjecture [32], that regardless what the degree of the MRS is, we have a similar result as [40, Theorem 1.1] for $n = 4p$ (p prime), or squarefree integers n, which along with our Theorem 5.2 would enable one to count, or at least estimate the equivalence classes of any degree MRS in these cases.

7. A simple criterion for (non)equivalence

In this section we want to find a simple criterion to detect (non)equivalence between two given MRS. To that end, we consider matrix inverses and generalizations, but first a result on polynomials.

Lemma 7.1. *Let f be an MRS Boolean function, and F_i, $i = 1, 2$, be the generating polynomials for the circulant matrices $M_1 = \mathrm{C}(a_1, a_2, \ldots, a_n)$, respectively, $M_2 = \mathrm{C}(b_1, \ldots, b_n)$ in A_f, where $(b_1, \ldots, b_n) = \rho_n^k(a_1, \ldots, a_n)$, for some k. Then, $\gcd(F_1(z), z^n - 1) = \gcd(F_2(z), z^n - 1)$.*

Proof. Since $(b_1, b_2, \ldots, b_n) = \rho_n^k(a_1, a_2, \ldots, a_n)$, for some k, an inductive argument will show the lemma, if we can prove the claim for $k = 1$, namely, for $(b_1, b_2, \ldots, b_n) = (a_n, a_1, \ldots, a_{n-1})$. That is, for $F_1(z) = a_1 + a_2 z + \cdots + a_n z^{n-1}$ and $F_2(z) = a_n + a_1 z + \cdots + a_{n-1} z^{n-1}$, we need to show that $\gcd(F_1(z), z^n - 1) = \gcd(F_2(z), z^n - 1)$. Certainly, $zF_1(z) - F_2(z) = a_n(z^n - 1)$, and so, $\gcd(F_1(z), z^n - 1) = \gcd(zF_1(z), z^n - 1) = \gcd(a_n(z^n - 1) + F_2(z), z^n - 1) = \gcd(F_2(z), z^n - 1)$. The lemma is proved. □

The following result is simple to show and well-known (see, for instance, [4, Theorem 2.2], or [39], although the result appears much earlier [24]).

Theorem 7.2. *Let $A = \mathrm{C}(a_1, a_2, \ldots, a_n)$ be a binary circulant matrix with generating polynomial $F(z) = a_1 + a_2 z + \cdots + a_n z^{n-1} \in \mathbb{F}_2[z]$. If $\gcd(F, z^n - 1) = 1$, then the matrix A is invertible and its inverse is $A^{-1} = \mathrm{C}(\alpha_1, \ldots, \alpha_n)$, where $(\alpha_1, \alpha_2, \ldots, \alpha_n)$ is the unique solution of*

$$(\alpha_1, \alpha_2, \ldots, \alpha_n) \cdot A = (1, 0, \ldots, 0).$$

Moreover, if $F^*(z) = \sum_{j=1}^{n} \alpha_j z^{j-1}$, then $F(z) \cdot F^*(z) \equiv 1 \pmod{z^n - 1}$.

However, the situation when $\gcd(F, z^n - 1) \neq 1$ is not so easy. For a square matrix A, we call a matrix A^* (of the same dimension) a *generalized inverse* if $AA^*A = A$. Let $A^\dagger$ be the (binary) *reflexive generalized* matrix, which satisfies $AA^\dagger A = A$, $A^\dagger AA^\dagger = A^\dagger$. In addition, if both $AA^\dagger$, $A^\dagger A$ are symmetric, then $A^\dagger$ is called a *(Moore–Penrose) pseudoinverse* [1]. It is known [34] that matrices over finite fields have at least one generalized inverse, however, if the pseudoinverse exists, it is unique. Also, it is not known if any of these generalized inverses are circulant, and our first result of this section deals with this problem.

Theorem 7.3. *Let $A = \mathrm{C}(a_1, \ldots, a_n)$ be a circulant matrix over $\mathbb{F}_2$ of generating polynomial $F = \sum_{j=1}^{n} a_j z^{j-1} \in \mathbb{F}_2[z]$. Let $\gcd(F(z), z^n - 1) = D(z)$, $z^n - 1 = H(z) \cdot D(z)$, and assume that $\gcd(D(z), H(z)) = 1$. Then the polynomial F is invertible modulo H, that is, there exists $F^*(z) = \sum_{j=1}^{n} \alpha_j z^{j-1}$ with $F(z) \cdot F^*(z) \equiv 1 \pmod{H(z)}$. Moreover, the circulant matrix A has a circulant generalized inverse, precisely, $AA^*A = A$, where $A^* = \mathrm{C}(\alpha_1, \ldots, \alpha_n)$. If, further, $\gcd(F, z^n - 1) = \gcd(F^*, z^n - 1)$, then A^* is in fact the reflexive generalized inverse $A^\dagger$, that is, it also satisfies $A^*AA^* = A^*$.*

Proof. Let $n = 2^t m$ with m odd, and t an arbitrary integer. It is known that every irreducible factor of $z^n - 1$ (over $\mathbb{F}_2$) appears at the power 2^t. Let $\Phi(z)$ be an arbitrary irreducible factor of $H(z) = (z^n - 1)/D(z)$. Since $\gcd(D(z), H(z)) = 1$, then $\gcd(F(z), \Phi(z)) = 1$ and so, the class of $F(z)$ is invertible in the ring $\mathbb{F}_2[z]/\langle \Phi^{2^t} \rangle$, that is, there exists $F_\Phi(z)^*$ with $F(z) \cdot F_\Phi(z)^* \equiv 1 \pmod{\Phi^{2^t}}$. Using the fact that $H(z) = \prod_{\Phi \text{ distinct}} \Phi^{2^t}$, and applying the Chinese Remainder Theorem, we obtain that there exists F^* with $F(z) \cdot F^*(z) \equiv 1 \pmod{H(z)}$. Moreover, $F^*(z)$ is unique modulo $H(z)$.

To show the second claim of our theorem, we assume that $F \cdot F^* \equiv 1 \pmod{H}$, where $F^*(z) = \sum_{j=1}^{n} \alpha_j z^{j-1}$, and we will show that $AA^*A = A$, where $A^* = \mathrm{C}(\alpha_1, \ldots, \alpha_n)$.

Let R be the quotient ring $\mathbb{F}_2[z]/\langle H(z) \rangle$. Since D divides F and H divides $FF^* - 1$, then $z^n - 1 = HD$ divides $F(FF^* - 1)$ and so, we have the identity $F^2F^* = F$ in $\mathbb{F}_2[z]/\langle z^n - 1 \rangle$. Multiplying out the polynomials F^2, F^*, and reducing modulo $z^n - 1$, we obtain

$$\sum_{2i+k \equiv 3 \pmod{n}} a_i \alpha_k + \left(\sum_{2i+k \equiv 4 \pmod{n}} a_i \alpha_k \right) z + \cdots + \left(\sum_{2i+k \equiv 2 \pmod{n}} a_i \alpha_k \right) z^{n-1} = \sum_{\ell=1}^{n} a_\ell z^{\ell-1},$$

which implies the corresponding circulant matrices are equal, thus $AA^*A = A$.

Using $\gcd(F(z), z^n - 1) = \gcd(F^*(z), z^n - 1)$, by a similar argument as before, we get that A is also a generalized inverse for A^*, that is, $A^*AA^* = A^*$, which shows the last claim of our theorem. □

Remark 7.4. Although there are plenty of generalized inverses (many of which are circulant) in general, we want to point out that by Theorem 7.3 the polynomials associated to these generalized inverses are all congruent modulo the corresponding H. Further, if the associated polynomial F is invertible modulo H, then A has a generalized inverse, but the converse may not be true.

What about the symmetry of AA^* (needed for pseudoinverse)? Multiplying the circulant matrices and transposing shows that having A and A^* circulant does not necessarily imply that $AA^* = (AA^*)^T$ holds, in general.

Remark 7.5. It may be tempting to conjecture that every circulant matrix has a generalized inverse that is circulant. However, that is not so, if $gcd(D, H) \neq 1$. For example, let $n = 6$, and $F(z) = 1 + z^3$. Since $z^6 - 1 = F(z)^2$, then (with the previous notations) $H(z) = D(z) = F(z)$, and consequently F has no inverse modulo F. One can also easily check (as we did, using a computer program) that the circulant matrix $\mathrm{C}(1, 0, 0, 1, 0, 0)$ corresponding to $F(z) = 1 + z^3$ has no circulant generalized inverse.

Regarding the singularity (or nonsingularity) of the associated circulant matrix to an MRS, we recall the following result [38,24], which gives a characterization of Boolean functions whose associated circulant matrices are singular (nonsingular).

Proposition 7.6. *Let f be a degree d MRS with associated $A_f = \langle C(a_1, \ldots, a_n)\rangle$ (assume that $a_1 = 1$). Let $\Delta(A_f) = \{1, s_2, \ldots, s_d\}$. Then A_f is singular if and only if there is an nth root of unity μ such that $1 + \mu^{s_2} + \cdots + \mu^{s_d} = 0$ (over $\mathbb{F}_2$).*

As a corollary, one gets easily the next result, also a consequence of [38, Lemma 3].

Corollary 7.7. *With the notations of the previous proposition, we have:*

(i) *If $wt(\Delta(A_f))$ is even, then A_f is singular.*
(ii) *Let p be the least odd prime occurring in the factorization of n. Assume that $\Delta(A_f) = \{1, s_2, \ldots, s_d\}$ has odd weight d and $s_d \le p - 2$. Then A_f is nonsingular.*

For a degree d MRS f with invertible class A_f, we let $\Delta(A_f^{-1}) = \{j_1, j_2, \ldots, j_t\}$ and we define the MRS *dual function* f^* by

$$f^* = x_{j_1}x_{j_2}\cdots x_{j_t} + x_{j_1+1}x_{j_2+1}\cdots x_{j_t+1} + \cdots + x_{j_1-1}x_{j_2-1}\cdots x_{j_t-1}.$$

Our next result gives a (necessary, but not sufficient) extension for higher degrees of Theorem 2.1.

Theorem 7.8. *Let f, g be two MRS Boolean functions in n-variables. If $f \overset{S}{\sim} g$ (i.e., f, g are affine equivalent by a permutation in S_n) and A_f is invertible, then A_g is also invertible, and the corresponding dual functions f^*, g^* are S-equivalent. Hence $wt(\Delta(f)) = wt(\Delta(g))$ and $wt(\Delta(f^*)) = wt(\Delta(g^*))$.*

Proof. Let A, B be representative circulant matrices of the classes A_f, A_g, respectively. From Theorem 5.2, there are permutation matrices P, Q such that $PA = BQ$. Since A, P, Q are invertible, their determinants are all 1 (mod 2), and thus so is $\det(B)$. Taking the inverse gives $A^{-1}P^T = Q^TB^{-1}$, or $QA^{-1} = B^{-1}P$. Then, again by Theorem 5.2, $f^* \overset{S}{\sim} g^*$ and so have equal degree. In terms of the weights of rows of the matrices, if $A = C(\mathbf{a})$, $B = C(\mathbf{b})$, $A^{-1} = C(\boldsymbol{\alpha})$, $B^{-1} = C(\boldsymbol{\beta})$, then $wt(\mathbf{a}) = wt(\mathbf{b})$ and $wt(\boldsymbol{\alpha}) = wt(\boldsymbol{\beta})$, and the theorem is shown. □

Remark 7.9. Note that any bit vector may be permuted to give any other of the same weight, so for the above vectors, some permutation takes $\mathbf{a}$ to $\mathbf{b}$ and another takes $\boldsymbol{\alpha}$ to $\boldsymbol{\beta}$.

Example 7.10. Take $n = 5$, and $f \overset{S}{\sim} g$ whose SANFs are $x_1x_2x_4$, respectively, $x_1x_2x_3$ (and so, $wt(\Delta(f)) = wt(\Delta(g))$). Certainly,

$$A_f = \langle C(1,1,0,1,0)\rangle, \quad A_g = \langle C(1,1,1,0,0)\rangle;$$
$$A_f^{-1} = \langle C(1,1,1,0,0)\rangle, \quad A_g^{-1} = \langle C(1,1,0,1,0)\rangle$$

and so, $wt(\Delta(f^*)) = wt(\Delta(g^*))$ (in fact, in this case the dual of f is $f^* = g$). As another example, we take $n = 8, f, g$ with SANFs $x_1x_2x_4$, respectively, $x_1x_2x_6$ (and so, $wt(\Delta(f)) = wt(\Delta(g))$). We compute

$$A_f = \langle C(1,1,0,1,0,0,0,0)\rangle, \quad A_g = \langle C(1,1,0,0,0,1,0,0)\rangle;$$
$$A_f^{-1} = \langle C(1,1,1,1,0,1,0,0)\rangle, \quad A_g^{-1} = \langle C(1,1,0,0,0,1,0,0)\rangle,$$

and so, $wt(\Delta(f^*)) = 5 \neq wt(\Delta(g^*)) = 3$, therefore $f \overset{S}{\not\sim} g$.

Remark 7.11. The conditions $wt(\Delta(f)) = wt(\Delta(g))$, $wt(\Delta(f^*)) = wt(\Delta(g^*))$ are not sufficient to ensure that the functions f, g are S-equivalent. As an example, take $n = 8$ and f, g with $\Delta(f) = \{1, 2, 3\}$, $\Delta(g) = \{1, 2, 4\}$. The two functions are not in the same S-equivalence class, yet $wt(\Delta(f)) = wt(\Delta(g)) = 3$ and $wt(\Delta(f^*)) = wt(\Delta(g^*)) = 5$, as one can check easily.

For a degree d MRS, whose class A_f is not invertible, let the equivalence class of the pseudoinverse (also circulant) matrix denoted by $A_f^\dagger$ (if it exists, it is unique) with $\Delta(A_f^\dagger) = \{j_1, j_2, \ldots, j_t\}$. Then the *pseudo-dual Boolean function* is

$$f^\dagger = x_{j_1}x_{j_2}\cdots x_{j_t} + x_{j_1+1}x_{j_2+1}\cdots x_{j_t+1} + \cdots + x_{j_1-1}x_{j_2-1}\cdots x_{j_t-1}.$$

By abuse of notation, we let $wt(\Delta(f^\dagger)) := wt(A_f^\dagger)$. We propose the following question, which seems to be true (supported by a lot of computer data).

Open Problem. *If $f \overset{S}{\sim} g$ with singular matrices A_f, A_g admitting circulant pseudoinverses, is it true that $wt(\Delta(f)) = wt(\Delta(g))$ and $wt(\Delta(f^\dagger)) = wt(\Delta(g^\dagger))$?*

While we cannot answer this open question at this moment, we can certainly give some necessary condition for the S-equivalence (assuming the existence of pseudoinverses).

Theorem 7.12. *Let f, g be two n-variable MRS functions with $f \overset{S}{\sim} g$, and $A_f = \langle \mathrm{C}(a_1, \ldots, a_n)\rangle$, $A_g = \langle \mathrm{C}(a_{\pi(1)}, \ldots, a_{\pi(n)})\rangle$ (for some permutation π), whose pseudoinverses are $\langle \mathrm{C}(\alpha_1 \ldots, \alpha_n)\rangle$, $\langle \mathrm{C}(\beta_1, \ldots, \beta_n)\rangle$. Let τ be the permutation $\tau(1) = 1$, $\tau(2) = \lceil n/2\rceil + 1$, $\tau(3) = 2$, $\tau(4) = \lceil n/2\rceil + 2, \ldots$. The following statements are true:*

(i) *Let n be odd. Then*

$$
\begin{aligned}
(a_1, \ldots, a_n) &= \left(a_{\tau(1)}, \ldots, a_{\tau(n)}\right) \mathrm{C}(\alpha_1, \ldots, \alpha_n)\\
(\alpha_1, \ldots, \alpha_n) &= \left(\alpha_{\tau(1)}, \ldots, \alpha_{\tau(n)}\right) \mathrm{C}(a_1, \ldots, a_n)\\
\left(a_{\pi(1)}, \ldots, a_{\pi(n)}\right) &= \left(a_{(\pi\circ\tau)(1)}, \ldots, a_{(\pi\circ\tau)(n)}\right) \mathrm{C}(\beta_1, \ldots, \beta_n)\\
(\beta_1, \ldots, \beta_n) &= \left(\beta_{\tau(1)}, \ldots, \beta_{\tau(n)}\right) \mathrm{C}\left(a_{\pi(1)}, \ldots, a_{\pi(n)}\right).
\end{aligned}
$$

(ii) *Let n be even. Then*

$$
\begin{aligned}
(a_1, \ldots, a_n) &= \left(a_{\tau(1)} + a_{\tau(2)}, 0, a_{\tau(3)} + a_{\tau(4)}, 0, \ldots\right) \mathrm{C}(\alpha_1, \ldots, \alpha_n)\\
(\alpha_1, \ldots, \alpha_n) &= \left(\alpha_{\tau(1)} + \alpha_{\tau(2)}, 0, \alpha_{\tau(3)} + \alpha_{\tau(4)}, 0, \ldots\right) \mathrm{C}(a_1, \ldots, a_n)\\
\left(a_{\pi(1)}, \ldots, a_{\pi(n)}\right) &= \left(a_{(\pi\circ\tau)(1)} + a_{(\pi\circ\tau)(2)}, 0, \ldots\right) \mathrm{C}(\beta_1, \ldots, \beta_n)\\
(\beta_1, \ldots, \beta_n) &= \left(\beta_{\tau(1)} + \beta_{\tau(2)}, 0, \ldots, \right) \mathrm{C}\left(a_{\pi(1)}, \ldots, a_{\pi(n)}\right).
\end{aligned}
$$

Proof. The proof is straightforward, using the commutativity of circulant matrices, but rather tedious. □

For an MRS f, if A_f does not have a pseudoinverse, rather only circulant generalized inverses, then the notion of dual is not well-defined, since the weights of the (usually, more than one) generalized inverses differ. One might choose the first in lexicographical order for the dual f^*, or allow multiple duals. Using this notion, for singular A_f, A_g without a pseudoinverse, rather only circulant generalized inverses, the condition $wt(\Delta(f^*)) = wt(\Delta(g^*))$ is not necessary (as in Theorem 7.8).

As an example for $n = 7$, let f have SANF $x_1x_2x_3x_5$ and g have SANF $x_1x_2x_3x_6$, where $f \overset{S}{\sim} g$ (from [12, Table 1]). We computed all generalized inverses that are circulant, all of which correspond (via the congruence modulo the corresponding H's — see Remark 7.4) to $A_f^* = \langle \mathrm{C}(1, 0, 0, 0, 0, 0, 0)\rangle$, $A_g^* = \langle \mathrm{C}(1, 1, 0, 0, 0, 0, 0)\rangle$ (smallest in lexicographical order), which clearly do not satisfy $wt(\Delta(f^*)) = wt(\Delta(g^*))$.

Acknowledgments

We thank the referees for a careful reading of the paper and for comments which improved its quality. We also thank Prof. T.W. Cusick for useful discussions and for pointing out Ref. [24].

References

[1] B.-I. Adi, T.N.E. Greville, Generalized Inverses, Springer–Verlag, 2003.
[2] E.R. Berlekamp, L.R. Welch, Weight distribution of cosets of the (32, 6) Reed–Muller code, IEEE Trans. Inform. Theory 18 (1972) 203–207.
[3] M.L. Bileschi, T.W. Cusick, D. Padgett, Weights of Boolean cubic monomial rotation symmetric functions, Cryptography Commun. 4 (2) (2012) 105–130.
[4] D. Bini, G.M. Del Corso, G. Manzini, L. Margara, Inversion of circulant matrices over $\mathbb{Z}_m$, Math. Comp. 70 (2001) 1169–1182.
[5] A. Biryukov, C. De Cannière, A. Braeken, B. Preneel, A toolbox for cryptanalysis: Linear and affine equivalence algorithms, in: E. Biham (Ed.), Advances in Cryptology – Eurocrypt, in: LNCS, vol. 2656, Springer–Verlag, 2003, pp. 33–50.
[6] A. Braeken, Y. Borissov, S. Nikova, B. Preneel, Classification of Boolean functions of 6 variables or less with respect to some cryptographic properties, in: Automata, Languages and Programming, in: LNCS, vol. 3580, Springer, Berlin, 2005, pp. 324–334. Longer version at http://eprint.iacr.org/2004/248.
[7] A. Brown, T.W. Cusick, Equivalence classes for cubic rotation symmetric functions, Cryptogr. Commun. 5 (2) (2013) 85–118.
[8] C. Carlet, Correlation-immune Boolean functions for leakage squeezing and rotating s-box masking against side channel attacks, in: Security, Privacy, and Applied Cryptography Engineering, in: LNCS, vol. 8204, 2013, pp. 70–74.
[9] J. Clark, J. Jacob, S. Maitra, P. Stănică, Almost Boolean functions: The design of Boolean functions by spectral inversion, Comput. Intell. 20 (2004) 450–462.
[10] T.W. Cusick, Affine equivalence of cubic homogeneous rotation symmetric functions, Inform. Sci. 181 (22) (2011) 5067–5083.
[11] T.W. Cusick, A. Brown, Affine equivalence for rotation symmetric Boolean functions with p^k variables, Finite Fields Appl. 18 (3) (2012) 547–562.
[12] T.W. Cusick, Y. Cheon, Affine equivalence of quartic homogeneous rotation symmetric Boolean functions, Inform. Sci. 259 (2014) 192–211.
[13] T.W. Cusick, Y. Cheon, Affine equivalence for rotation symmetric Boolean functions with 2^k variables, Des. Codes Cryptogr. 63 (2012) 273–294.
[14] T.W. Cusick, Y. Cheon, Affine equivalence for cubic rotation symmetric Boolean functions with $n = pq$ variables, Discrete Math. 327 (2014) 51–61.
[15] T.W. Cusick, P. Stănică, Fast evaluation, weights and nonlinearity of rotation-symmetric functions, Discrete Math. 258 (2002) 289–301.
[16] D.K. Dalai, K.C. Gupta, S. Maitra, Cryptographically significant Boolean functions: Construction and analysis in terms of algebraic immunity, in: H. Gilbert, H. Handschuh (Eds.), Fast Software Encryption, in: LNCS, vol. 3557, 2005, pp. 98–111.
[17] D.K. Dalai, K.C. Gupta, S. Maitra, Results on algebraic immunity for cryptographically significant Boolean functions, in: Proceedings of Indocrypt 2004, in: LNCS, vol. 3348, 2004, pp. 92–106.
[18] P.J. Davis, Circulant Matrices, John Wiley and Sons, New York, 1979.
[19] E. Filiol, C. Fontaine, Highly nonlinear balanced Boolean functions with a good correlation-immunity, in: Adv. in Crypt. - EUROCRYPT'98, in: LNCS, vol. 1403, Springer-Verlag, 1998, pp. 475–488.
[20] J.E. Fuller, Analysis of affine equivalent Boolean functions for cryptography (Ph.D. thesis), Information Security Research Centre, Queensland Univ. Tech, 2003.
[21] J.E. Fuller, W. Millan, Linear redundancy in S-boxes, in: Fast Software Encryption 2003, in: LNCS, vol. 2887, Springer, Berlin, 2003, pp. 74–86.
[22] M.A. Harrison, On the classification of Boolean functions by the general linear and affine groups, J. Soc. Indust. Appl. Math. (1964) 285–299.

[23] M. Hell, A. Maximov, S. Maitra, On efficient implementation of search strategy for rotation symmetric Boolean functions, in: Ninth International Workshop on Algebraic and Combinatoral Coding Theory, ACCT 2004, June 19–25, 2004, Black Sea Coast, Bulgaria.
[24] A.W. Ingleton, The rank of circulant matrices, J. Lond. Math. Soc. s1-31 (4) (1956) 445–460.
[25] S. Kavut, S. Maitra, M.D. Yücel, Enumeration of 9-variable rotation symmetric Boolean functions having nonlinearity >240, in: Adv. in Crypt. – Indocrypt 2006, in: LNCS, vol. 4329, Springer, Berlin, 2006, pp. 266–279.
[26] S. Kavut, S. Maitra, M.D. Yücel, Search for Boolean functions with excellent profiles in the rotation symmetric class, IEEE Trans. Inform. Theory 53 (2007) 1743–1751.
[27] S. Kavut, M.D. Yücel, Generalized rotation symmetric and dihedral symmetric Boolean functions - 9 variable Boolean functions with nonlinearity 242, in: Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC 2007, in: LNCS, vol. 4851, 2007, pp. 321–329.
[28] K.V. Lakshmy, M. Sethumadhavan, T.W. Cusick, Counting rotation symmetric functions using Polya's theorem, Discrete Appl. Math. 169 (2014) 162–167.
[29] J.A. Maiorana, A classification of cosets of the Reed–Muller code $R(1, 6)$, Math. Comp. 57 (1991) 403–414.
[30] A. Maximov, Classes of plateaued rotation symmetric Boolean functions under transformation of Walsh spectra, in: O. Ytrehus (Ed.), Workshop on Coding and Cryptology 2005, in: LNCS, vol. 3969, 2006, pp. 325–334.
[31] A. Maximov, M. Hell, S. Maitra, Plateaued rotation symmetric Boolean functions on odd number of variables, in: International Workshop on Boolean Functions: Cryptography and Applications, BFCA 2005, University of Rouen, France, 2005, available at eprint.iacr.org no. 2004/144, 2004.
[32] M. Muzychuk, On Ádám's conjecture for circulant graphs, Discrete Math. 176 (1–3) (1997) 285–298.
[33] N.J. Patterson, D.H. Wiedemann, The covering radius of the $(2^{15}, 16)$ Reed–Muller code is at least 16276, IEEE Trans. Inform. Theory 29 (1983) 354–356; See also the correction in IEEE Trans. Inform. Theory 36 (1990) 443.
[34] M.H. Pearl, Generalized inverses of matrices with entries taken from an arbitrary field, Linear Algebra Appl. 1 (1968) 571–587.
[35] J. Pieprzyk, C.X. Qu, Fast hashing and rotation-symmetric functions, J. UCS 5 (1999) 20–31.
[36] V. Rijmen, P.S.L.M. Barreto, D.L.G. Filho, Rotation symmetry in algebraically generated cryptographic substitution tables, Inform. Process. Lett. 106 (2008) 246–250.
[37] P. Stănică, S. Maitra, Rotation symmetric Boolean functions – count and cryptographic properties, Discrete Appl. Math. 156 (2008) 1567–1580.
[38] P. Stănică, S. Maitra, J. Clark, Results on rotation symmetric Bent and correlation immune Boolean functions, in: Fast Software Encryption Workshop, FSE 2004, in: LNCS, vol. 3017, Springer Verlag, New Delhi, India, 2004, pp. 161–177.
[39] J.-Q. Wang, C.-Z. Dong, Inverse matrix of symmetric circulant matrix on skew field, Int. J. Algebra 1 (11) (2007) 541–546.
[40] D. Wiedemann, M.E. Zieve, Equivalence of sparse circulants: the bipartite Ádám problem, in: IACR Cryptology ePrint Archive, 2007, arxiv.org/pdf/0706.1567.